RGPD:
che cosa occorre sapere?

SHL.

1 - Introduzione

Da sempre qualità di leader globale nella fornitura di soluzioni di assessment di talenti, rivolgiamo particolare attenzione alla protezione delle informazioni personali affidateci dalla nostra clientela. È per noi d'importanza capitale garantire la conformità con leggi e normative applicabili nel campo della protezione dei dati.

Questa dichiarazione presenta informazioni in merito alla nostra conformità, nonché ai programmi volti a supportare la conformità dei clienti, al Regolamento generale sulla protezione dei dati (RGPD), entrato in vigore il 25 maggio 2018. In qualità di responsabili del trattamento dei dati possiamo vantare una comprovata esperienza in termini di sicurezza dei dati e di prassi solide ed affidabili.

Con costanza e dedizione ci adoperiamo per garantire la conformità al RGPD, come indicato più nel dettaglio nella sezione 3, adottando un approccio di miglioramento continuo.

2 - RGPD: significato e rilevanza per il cliente

Il RGPD (in inglese GDPR - General Data Protection Regulation) e il Data Protection Act 2018, emanato nel Regno Unito, rappresentano un cambiamento significativo della legislazione sulla protezione dei dati, sia nell'Unione europea sia nel Regno Unito, che comporta diversi effetti sui nostri servizi e sui nostri clienti; elenchiamo di seguito i cambiamenti più rilevanti.

- **Responsabilità:** ai sensi del RGPD, il nuovo principio di responsabilità prevede che le organizzazioni dimostrino in modo più esplicito la conformità ai principi del suddetto regolamento.
- **Estensione dei diritti individuali:** ai diritti individuali (diritti di accesso, rettifica, opposizione al trattamento dei dati e limitazione del trattamento) si aggiungono il diritto di cancellazione e il diritto alla portabilità dei dati per ciascun soggetto interessato.
- **Quadro di governance:** direttamente correlato al principio di responsabilità summenzionato, definisce l'obbligo, da parte di titolari e responsabili del trattamento dei dati, di attuare misure tecniche e organizzative appropriate per garantire e dimostrare la conformità al RGPD di tutti i trattamenti di dati personali.
- **Sanzioni:** le autorità di vigilanza degli Stati membri dell'UE e l'Ufficio del Commissario per le Informazioni del Regno Unito (responsabili per l'applicazione del RGPD) possono imporre sanzioni fino al 4% del fatturato globale o altrimenti pari a € 20.000.000, a seconda di quale sia l'importo più elevato, per eventuali violazioni del RGPD.

3 - Perché lavorare con noi

Diamo priorità alla sicurezza delle informazioni: ben prima dell'entrata in vigore del RGPD, abbiamo sempre considerato la salvaguardia dei dati personaliun elemento cardine della propria attività. Il nostro impegno per la sicurezza è attestato dai nostri programmi di certificazione in corso, attivi ormai da anni. In particolare, abbiamo sviluppato e implementato da oltre dieci anni un sistema di gestione della sicurezza delle informazioni con certificazione ISO 27001. Inoltre, abbiamo ottenuto la certificazione ISO 22301 per le nostre Pratiche di Continuità Operativa e le certificazioni ISO 20000 grazie alla capacità di mantenimento, supporto e gestione professionali dei nostri servizi informatici implementando le best practice.

Abbiamo adottato tutte le misure necessarie. Al fine di ottemperare al RGPD, abbiamo adottato le seguenti misure in modo da irrobustire ulteriormente i nostri sistemi di protezione dei dati.

- **Aggiornamento di politiche e procedure:** al fine di garantire la conformità al RGPD abbiamo provveduto a rivedere ed aggiornare le nostre politiche e procedure già in essere. Ogni membro dello staff e tutte le figure chiave del nostro organigramma ricevono costantemente un'adeguata formazione su queste politiche, in modo da garantire la nostra conformità ed offrirviassistenza per i vostri impegni di conformità.
- **Aggiornamento dell'informativa sulla protezione dei dati:** la nostra informativa corrente sulla protezione dei dati presentata ai candidati quando si sottopongono ad una procedura di assessment è conforme ai requisiti del RGPD.
- **Aggiornamento degli accordi in materia di trattamento dei dati:** abbiamo aggiornato gli accordi stipulati con i nostri clienti integrando specifiche disposizioni al fine di garantirne la conformità con i requisiti del RGPD.
- **Privacy by design and default:** ci impegniamo ad agevolare le strategie di governance nell'ambito della protezione dei dati dei nostri clienti, compresi i nuovi obblighi prescritti in base ai principi di privacy by design

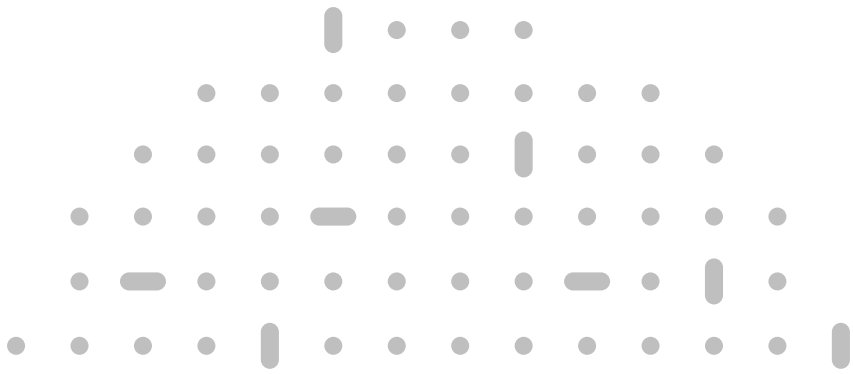
e privacy by default. Il concetto di "privacy by design" prevede che le organizzazioni adottino misure appropriate per integrare i principi di protezione dei dati del RGPD nelle rispettive attività tenendo conto di costi, rischi e contesto operativo. Il concetto di "privacy by default" prevede invece che le organizzazioni, come condizione predefinita, adottino misure tecniche ed organizzative appropriate per ridurre al minimo l'utilizzo dei dati per ciascuna delle finalitàper lequali vengono raccolti.

- **Avviso di violazione dei dati personali:** ai sensi del RGPD sussiste l'obbligo di informare l'autorità di vigilanza senza indebito ritardo e, ove possibile, non oltre 72 ore dopo essere venuti a conoscenza di una violazione dei dati personali. Nel caso in cui veniamo a conoscenza di una violazione che riguarda i dati personali, provvediamo ad informare il cliente senza indebito ritardo entro e non oltre 48 ore, aiutandolo ad ottemperare ai suoi obblighi ai sensi del RGPD e fornendogli tempestivamente le informazioni richieste in relazione alla suddetta violazione.
- **Assessment dell'impatto sulla privacy:** è nostro impegno aiutare il cliente ad adempiere ai suoi obblighi ai sensi del RGPD, mettendo a disposizione procedure di assessment dell'impatto sulla privacy al fine di identificare e ridurre al minimo il rischio di non conformità.
- **Monitoraggio della conformità al RGPD:** sottoponiamo costantemente a verifiche ed ispezioni periodiche il livello di sicurezza dei nostri servizi e la nostra conformità a politiche e procedure ai sensi del RGPD.
- **Formazione:** forti di un programma di lunga data inerente alla formazione in materia di protezione dei dati, continueremo a formare il nostro personale a livello globale sui requisiti necessari in tale ambito, incluso il RGPD, nel contesto della nostra certificazione ISO 27001. Inoltre, offriamo una formazione più estesa alle figure chiave della nostra organizzazione come previsto dal RGPD.
- **Mantenimento dei registri delle attività di trattamento:** come previsto dal RGPD in qualità di responsabile del trattamento dei dati, mantieniamo un registro delle attività di trattamento per ciascuna tipologia di trattamento dei dati effettuata.
- **Assessment dei diritti individuali:** ai sensi del RGDP il cliente, in qualità di titolare del trattamento, è tenuto ad agevolare i diretti interessati nell'esercizio dei propri diritti. Da parte nostra , in qualità di responsabile del trattamento dei dati per conto del cliente, abbiamo definito specifiche modalità in base alle quali i nostri sistemi e processi possono aiutarvi nell'adempimento dei propri obblighi nei confronti degli interessati.

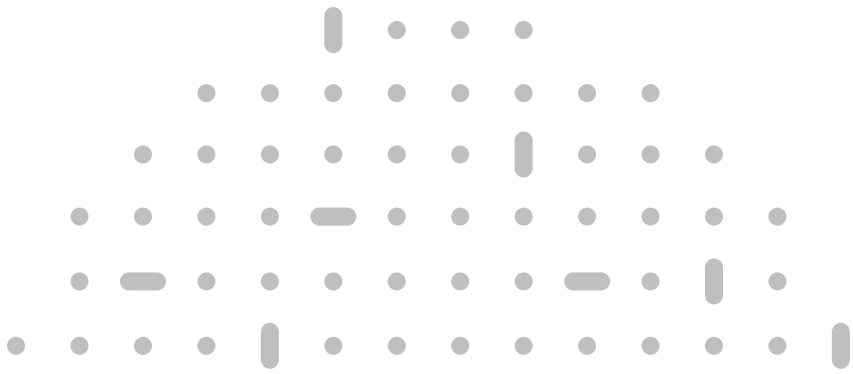
Articolo RGPD	Conformità
Articolo 13 **Diritto all'informazione**	La nostra piattaforma di assessment prevede l'invio preventivo di un avviso sulla protezione dei dati ai candidati che si sottopongono ad una procedura di assessment. Tale avviso fornisce alla persona interessata informazioni sulla raccolta e sul trattamento dei dati da parte della nostra azienda in ottemperanza ai requisiti della legislazione in materia di protezione dei dati. Poiché l'assessment costituisce solo una parte di un processo di reclutamento più ampio e non rappresenta di norma il primo punto di raccolta dei dati di un candidato, è possibile che i requisiti di informazione di cui all'Articolo 13 debbano essere soddisfatti ancor prima di avvalersi della piattaforma di assessment. È possibile utilizzare diversi metodi, ad esempio il sito web dedicato alle offerte di lavoro, un modulo di candidatura online o un sistema di tracciamento in grado di accogliere le candidature iniziali e acquisire altre informazioni personali (curriculum vitae, indirizzo di residenza ecc.). In ciascuno di questi sistemi, al momento della raccolta dei dati è necessario notificare un avviso sulla protezione dei dati che contempli l'intero ciclo di reclutamento. In tal senso, invitiamo i nostri clienti ad avvalersi di un consulente legale indipendente per verificare gli obblighi di conformità ai sensi dell'articolo 13 del RGPD.

Articolo RGPD	Conformità
Articoli 15 - 18 **Diritto di** **• accesso** **• rettifica** **• cancellazione** **• limitazione del trattamento**	La richiesta di un candidato di accedere, correggere, cancellare o limitare il trattamento dei dati deve essere indirizzata al cliente in qualità di titolare del trattamento. Talvolta riceviamo richieste direttamente dai candidati, i quali ci invitano a cancellare le loro informazioni o a fornire l'accesso ai risultati dei rispettivi assessment. Quando ciò accade, provvediamo a reindirizzare le suddette richieste al titolare del trattamento. Successivamente, forniamo al cliente assistenza e informazioni affinché possa assolvere i propri obblighi nei confronti del candidato. Se riceviamo tale richiesta direttamente dal cliente, abbiamo già predisposto processi atti a soddisfarla, sia che si tratti di rispondere tempestivamente a un'istanza di accesso del soggetto interessato o di acconsentire alla cancellazione dei suoi dati. Spesso i clienti ci chiedono informazioni sui nostri tempi di conservazione dei dati. In qualità di responsabile del trattamento dei dati, manteniamo in archivio le informazioni in conformità con gli accordi stipulati con i clienti, ragion per cui provvediamo a cancellarle previa richiesta da parte dei clienti medesimi. Nell'ambito della nostra strategia di conformità al RGPD abbiamo apportato miglioramenti alla nostra piattaforma al fine di incrementare

Articolo RGPD	Conformità
Articolo 20 **Diritto alla portabilità dei dati**	Il diritto alla portabilità dei dati si applica esclusivamente: • ai dati personali che una persona fisica (ossia un candidato) ha fornito ad un nostro cliente in qualità di titolare del trattamento; • laddove il trattamento sia vincolato al consenso del diretto interessato o volto all'esecuzione di un contratto; • laddove il trattamento venga eseguito tramite mezzi automatizzati (non si applica dunque ai registri cartacei). Dato l'ambito di applicazione dei prodotti e dei servizi offerti dalla nostra azienda, riteniamo che tale diritto sia strettamente correlato al diritto di accesso menzionato in precedenza. Pertanto, provvederemo a inoltrare le richieste al cliente interessato in qualità di titolare del trattamento, assistendolo successivamente nell'adempimento degli obblighi di conformità. Le informazioni raccolte direttamente da un soggetto sono limitate, ragion per cui è possibile fornirle in un "formato strutturato, di uso comune, leggibile da una macchina e interoperabile" vagliando caso per caso. Spetta al cliente, in qualità di titolare del trattamento, determinare la portata delle informazioni che desidera rendere disponibili in base al diritto in questione.



Articolo RGPD	Conformità
Articolo 21 **Diritto di opposizione**	Un candidato può esercitare il diritto di opposizione all'elaborazione dei suoi dati personali nel caso in cui il titolare del trattamento dei dati invochi interessi legittimi come base giuridica del trattamento medesimo. Ciascun candidato ha facoltà di decidere se sottoporsi o meno a una prova di assessment. Nel caso in cui si opponga al trattamento dei dati, può semplicemente uscire dall'assessment, con conseguente interruzione del processo di trattamento da parte nostra. Nel caso in cui il candidato si opponga dopo aver già avviato la procedura di assessment, ciò determinerà la maturazione del diritto di cancellazione di cui all'articolo 1515 15
Articolo 22 **Diritti correlati ai processi automatizzati di decisione e profilazione**	Il RGPD sancisce il diritto di ciascun individuo a non essere oggetto di decisioni automatizzate, fatte salve specifiche clausole di esenzione. Spesso la nostra clientela si avvale dei nostri servizi come strumento decisionale nell'ambito del reclutamento di nuovo personale o della promozione dei dipendenti già in organico. Secondo le nostre linee guida sulle best practice, l'utilizzo dei nostri assessment è da intendersi come integrativo rispetto a procedure di valutazione più ampie e non deve costituire l'unica discriminante per decisioni relative ad un impiego. Per qualsiasi altro utilizzo dei nostri assessment, consigliamo di richiedere una consulenza legale indipendente sugli obblighi di conformità ai sensi dell'articolo 22 del RGPD. In qualità di titolare del trattamento dei dati, laddove il cliente ci comunichi la sua intenzione di utilizzare i nostri assessment come parte di un processo decisionale automatizzato, seguiremo le sue istruzioni e ci conformeremo al suo approccio rispetto alle eccezioni consentite, inoltrando ad esempio una notifica opportunamente formulata ai soggetti che potrebbero essere sottoposti a decisioni automatizzate.



Rispettiamo le regole di trasferimento internazionale: in conformità con la nostra prassi attuale, continueremo a garantire il nostro impegno a non trasferire informazioni al di fuori del SEE in assenza di un'adeguata struttura di trasferimento dei dati. Il nostro operato è attualmente vincolato dalle clausole contrattuali standard dell'UE (le cosiddette "clausole modello") in vigore per i trasferimenti al di fuori del SEE. A seguito delle domande frequenti del Comitato europeo per la protezione dei dati (EDPB - European Data Protection Board) adottate il 23 luglio 2020 (disponibili qui) in merito alla sentenza Schrems II, siamo lieti di fornire assistenza ai nostri clienti che desiderano adeguare la propria prassi operativa nell'ambito dei suddetti trasferimenti.

Abbiamo inoltre in corso l'aggiornamento delle nostre politiche e procedure alla luce del ritiro del Regno Unito dall'Unione Europea. Indipendentemente dalla Brexit, l'attività di SHL rimane tuttora vincolata al RGPD: al momento stiamo valutando possibili alternative per quanto concerne il trasferimento di dati tra il Regno Unito e il SEE.

Continueremo a monitorare qualsiasi modifica proposta alle clausole modello in base al RGPD e ci assicureremo di aggiornare di conseguenza gli accordi da noi proposti. Attendiamo inoltre ulteriori indicazioni dal Comitato Europeo per la Protezione dei Dati in merito a eventuali misure supplementari da adottare in caso di utilizzo delle clausole contrattuali standard dell'UE per il trasferimento di dati a paesi terzi.

Accordi sulla protezione dei dati: stipuliamo regolarmente accordi sulla protezione dei dati con i nostri clienti in base a quanto previsto dalle norme applicabili. Invitiamo i nostri clienti ad avvalersi del venditore di riferimento per contattarci e richiedere l'aggiornamento o l'implementazione delle clausole contrattuali standard dell'UE o di altri accordi legali in base alle loro esigen.

In caso di ulteriori domande è possibile rivolgersi all'account manager o inviare un'e-mail all'indirizzo di posta elettronica data.questions@shl.com.